IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

XYLON LICENSING LLC, Plaintiff, v. **WOODFOREST FINANCIAL GROUP, INC.,** Defendant.	Civil Action No.: 6:21-cv-00300 **TRIAL BY JURY DEMANDED**

COMPLAINT FOR INFRINGEMENT OF PATENT

Now comes, Plaintiff, Xylon Licensing LLC ("Plaintiff"), by and through undersigned counsel, and respectfully alleges, states, and prays as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement under the Patent Laws of the United States, Title 35 United States Code ("U.S.C.") to prevent and enjoin Defendant Woodforest Financial Group, Inc. (hereinafter "Defendant"), from infringing and profiting, in an illegal and unauthorized manner, and without authorization and/or consent from Plaintiff from U.S. Patent No 8,719,165 ("the '165 Patent" or the "Patent-in-Suit"), which is attached hereto as Exhibit A and incorporated herein by reference, and pursuant to 35 U.S.C. §271, and to recover damages, attorney's fees, and costs.

THE PARTIES

2. Plaintiff is a Texas limited liability company with its principal place of business at 6001 West Parmer Lane – Suite 370-1133, Austin, Texas 78727.

3. Upon information and belief, Defendant is a corporation organized under the laws of Texas, having a principal place of business at 25231 Grograns Mill Road – Suite 350, The Woodlands, Texas 77380. Upon information and belief, Defendant may be served with process

c/o James D. Dreibelbis, its Registered Agent, 25231 Grogans Mill Road – Suite 350, The Woodlands, Texas 77380.

4. Upon information and belief, Defendant owns, operates, or maintains a physical presence at 1030 Norwood Park Blvd, Austin, TX 78753, among others, which is in this judicial district.

JURISDICTION AND VENUE

5. This is an action for patent infringement in violation of the Patent Act of the United States, 35 U.S.C. §§1 *et seq*.

6. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§1331 and 1338(a).

7. This Court has personal jurisdiction over Defendant by virtue of its systematic and continuous contacts with this jurisdiction and its residence in this District, as well as because of the injury to Plaintiff, and the cause of action Plaintiff has risen in this District, as alleged herein.

8. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in this forum state and in this judicial District; and (iii) having a physical presence in the district.

9. Venue is proper in this judicial district pursuant to 28 U.S.C. §1400(b) because Defendant resides in this District under the Supreme Court's opinion in *TC Heartland v. Kraft Foods Group Brands LLC,* 137 S. Ct. 1514 (2017) through its incorporation, and regular and established place of business in this District.

FACTUAL ALLEGATIONS

10. On May 6, 2014, the United States Patent and Trademark Office ("USPTO") duly and legally issued the '165 Patent, entitled "DELEGATED TRANSACTIONS OVER MOBILE" after a full and fair examination. The '165 Patent is attached hereto as Exhibit A and incorporated herein as if fully rewritten.

11. Plaintiff is presently the owner of the '165 Patent, having received all right, title and interest in and to the '165 Patent from the previous assignee of record. Plaintiff possesses all rights of recovery under the '165 Patent, including the exclusive right to recover for past infringement.

12. To the extent required, Plaintiff has complied with all marking requirements under 35 U.S.C. § 287.

13. As identified in the '165 Patent, prior art systems were familiar with online purchases. See Ex. A at Col 1:6-9.

14. More particularly, the '165 Patent identifies that the prior art provided a scenario where a customer operates a full-featured and secure computing device to access a website operated by a merchant. Ex. A at Col. 1:10-11. The customer enters transaction data in a web-based form, and uses a website user interface to finalize the transaction. Ex. A at Col. 1:11-13. The merchant receives the transaction data, verifies payment, confirms that payment was received, confirms that the goods will be delivered accordingly, and subsequently delivers the goods. Ex. A at Col. 1:13-16.

15. Further, prior to the '165 Patent, electronic transactions using mobile devices were much less common than those using a fully featured laptop or desktop computer. Ex. A at Col. 2:10-14.

16. To address the limitations, the computer-centric or network-centric that resulted in a computing gap between smartphones and computers, the '165 Patent provided a system and method that generally relates to enabling completion of secure transactions using mobile devices that may or may not have appropriate security features needed or desired for the transaction. Ex. A at Col. 2:31-35. In some embodiments, a transaction may be partially completed by a secure computing device, and partially completed by a mobile device. Ex. A at Col. 2:35-37. The secure computing device can be arranged to delegate one or more transaction operation(s) to the mobile device. Ex. A at Col. 2:37-40. For example, a customer may initiate a transaction from a customer secure computing device, such as, for example, a secure personal computer (PC) in the customer's home or office. Ex. A at Col. 2:40-44. Instead of completing the transaction, however, the customer may delegate a transaction operation to a delegate mobile device. Ex. A at Col. 2:44-45. Upon receiving an appropriate communication from the delegate mobile device, the customer secure computing device may then complete the transaction. Ex. A at Col. 2:45-47. Similarly, a merchant may delegate transaction operation(s) to delegate mobile device(s). Ex. A at Col. 2:47-49.

17. To address this specific technical problem, Claim 1 in the '165 Patent comprises a non-abstract method for delegated transaction over mobile.

18. Particularly, Claim 1 of the '165 Patent provides:

> "1. A method for completing, by a customer secure computing device, a secure transaction between a customer and a merchant, wherein the customer is associated with the customer secure computing device and a delegate mobile device, the method comprising:
>
> acquiring customer delegate mobile device identification information and secure transaction data, by the customer secure computing device, comprising:
>
> receiving, by the customer secure computing device, secure transaction data associated with a delegated transaction, the secure transaction data comprising a merchant identification associated with the merchant;

receiving, by the customer secure computing device, customer delegate mobile device identification information associated with a customer delegate mobile device authorized by the customer for the delegated transaction with the merchant; and

storing, by the customer secure computing device, the secure transaction data and customer delegate mobile device identification information; and

subsequent to acquiring customer delegate mobile device identification information and secure transaction data by the customer secure computing device, automatically completing the secure transaction, by the customer secure computing device, in response to receiving a communication from the identified previously authorized customer delegate mobile device, comprising:

receiving, by the customer secure computing device, a communication from the identified previously authorized customer delegate mobile device;

checking, by the customer secure computing device, a status identifier in the communication from the identified previously authorized customer delegate mobile device; and

automatically initiating, by the customer secure computing device, using the secure transaction data, payment to the merchant by the customer secure computing device in response to receiving the communication from the identified previously authorized customer delegate mobile device, when the status identifier indicates that the delegated transaction is complete." See Exhibit A.

19. Claim 1 of the '165 Patent addressed the specific need for an improved delegated transaction over mobile or through mobile networks.

20. Specifically, to deal delegated mobile device, the method of Claim 1 in the '165 patent requires (a) receiving, by the customer secure computing device, *secure transaction data associated with a delegated transaction*, the secure transaction data comprising *a merchant identification associated with the merchant*; (b) receiving, by the customer secure computing device, customer delegate mobile device identification information associated with a customer delegate mobile device *authorized by the customer for the delegated transaction with the merchant*; (c) *subsequent* to acquiring customer delegate mobile device identification information

and secure transaction data by the customer secure computing device, *automatically completing the secure transaction*, by the customer secure computing device, *in response to receiving a communication from the identified previously authorized customer delegate mobile device*; and (d) receiving, and checking, by the customer secure computing device, a status identifier in the communication from the identified previously authorized customer delegate mobile device; and *automatically initiating*, by the customer secure computing device, *using the secure transaction data, payment to the merchant by the customer secure computing device in response to receiving the communication from the identified previously authorized customer delegate mobile device, when the status identifier indicates that the delegated transaction is complete*. These specific elements, as combined, accomplish the desired result improving the previous computer-centric or network-centric problems associated with delegated transactions over mobile device or through mobile networks.

21. Further, these specific elements also accomplish these desired results to overcome the then existing problems in the relevant field of network communication systems. *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018) (holding that improving computer security can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem). See also *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018); *Core Wireless Licensing v. LG Elecs., Inc.*, 880 F.3d 1356 (Fed. Cir. 2018); *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018); *Uniloc USA, Inc. v. LG Electronics USA, Inc.*, 957 F.3d 1303 (Fed. Cir. April 30, 2020).

22. Claims need not articulate the advantages of the claimed combinations to be eligible. *Uniloc USA, Inc. v. LG Elecs. USA, Inc.*, 957 F.3d 1303, 1309 (Fed. Cir. 2020).

23. These specific elements of Claim 1 of the '165 Patent were an unconventional arrangement of elements because the prior art methodologies would not use delegate transaction which made them less secure. By adding the specific elements of Claim 1 of the '165 Patent, an improved method was able to unconventionally complete a secure transaction. *Cellspin Soft, Inc. v. FitBit, Inc.*, 927 F.3d 1306 (Fed. Cir. 2019).

24. Further, regarding the specific non-conventional and non-generic arrangements of known, conventional pieces to overcome an existing problem, the method of Claim 1 in the '165 Patent provides a method of completing a secure transaction that would not preempt all ways of completing a transaction between a merchant and customer because completing the transaction is based on *authorization by the customer for the delegated transaction with the merchant*; *automatically completing the secure transaction*, by the customer secure computing device, *in response to receiving a communication from the identified previously authorized customer delegate mobile device*; and receiving, checking, by the customer secure computing device, a status identifier in the communication from the identified previously authorized customer delegate mobile device; and *automatically initiating*, by the customer secure computing device, *using the secure transaction data, payment to the merchant by the customer secure computing device in response to receiving the communication from the identified previously authorized customer delegate mobile device, when the status identifier indicates that the delegated transaction is complete*, any of which could be removed or performed differently to permit a method of gaining completing the secured transaction in a different way. *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016); See also *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014).

25. Based on the allegations, it must be accepted as true at this stage, that Claim 1 of the '165 Patent recites a specific, plausibly inventive way of completing a secure transaction and using specific protocols rather than the general idea of transacting between merchant and customer. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019), *cert. denied sub nom. Garmin USA, Inc. v. Cellspin Soft, Inc.*, 140 S. Ct. 907, 205 L. Ed. 2d 459 (2020).

26. Alternatively, there is at least a question of fact that must survive the pleading stage as to whether These specific elements of Claim 1 of the '165 Patent were an unconventional arrangement of elements. *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121 (Fed. Cir. 2018) See also *Berkheimer v. HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018), *cert. denied*, 140 S. Ct. 911, 205 L. Ed. 2d 454 (2020).

27. Defendant commercializes, inter alia, methods that perform all the steps recited in at least one claim of the '165 Patent. More particularly, Defendant commercializes, inter alia, methods that perform all the steps recited in Claim 1 of the '165 Patent. Specifically, Defendant makes, uses, sells, offers for sale, or imports a method that encompasses that which is covered by Claim 1 of the '165 Patent.

DEFENDANT'S PRODUCT(S)

28. Defendant offers solutions, such as SimpleSwipe, the SimpleSwipe App, CELL IT® Plus service, and a card reader (collectively the "Accused Product"),[1] that discloses a method for completing a secure transaction. A non-limiting and exemplary claim chart comparing the Accused Product of Claim 1 of the '165 Patent is attached hereto as Exhibit B and is incorporated herein as if fully rewritten.

[1] The Accused Product is just one of the products provided by Defendant, and Plaintiff's investigation is on-going to additional products to be included as an Accused Product that may be added at a later date.

29. As recited in Claim 1, a system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls a method for completing, by a customer secure computing device (e.g., card reader that is for a customer to use as they engage the card reader and insert a credit card to complete a purchase), a secure transaction (e.g., Data required to complete the delegated transaction such as Credit Card number, expiry date, CVV, details related to a merchant device such as device address to identify the merchant, etc. received in the encoded form) between a customer and a merchant, wherein the customer is associated with the customer secure computing device (e.g., card reader) and a delegate mobile device (e.g., Smartphone equipped with SimpleSwipe app connected to the card reader via Bluetooth). See Ex. B.

30. As recited in one step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls acquiring customer delegate mobile device identification information (e.g., Bluetooth address of the smartphone) and secure transaction data (e.g., Data required to complete the delegated transaction such as Credit Card number, expiry date, CVV, details related to the merchant device such as device address to identify the merchant, etc. received in the encoded form), by the customer secure computing device (e.g., card reader). See Ex. B.

31. As recited in another step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls receiving, by the customer secure computing device (e.g., card reader), secure transaction data (e.g., Data required to complete the delegated transaction such as Credit Card number, expiry date, CVV, details related to the merchant device such as device address to identify the merchant, etc. received in the encoded form) associated with a delegated transaction (e.g., current transaction or transaction in discussion), the secure transaction data (e.g., Data required to complete the delegated transaction

such as Credit Card number, expiry date, CVV, details related to the merchant device such as device address to identify the merchant, etc. received in the encoded form) comprising a merchant identification associated with the merchant (e.g., details related to the merchant device such as device address to identify the merchant). See Ex. B.

32. As recited in one step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls receiving, by the customer secure computing device (e.g., card reader), customer delegate mobile device identification information (e.g., Bluetooth address of the smartphone) associated with a customer delegate mobile device (e.g., Smartphone connected to the card reader via Bluetooth) authorized (e.g., by pairing it with the card reader) by the customer for the delegated transaction (e.g., current transaction or transaction in discussion) with the merchant. See Ex. B.

33. As recited in another step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls storing, by the customer secure computing device (e.g., card reader), the secure transaction data (e.g., Data required to complete the delegated transaction such as Credit Card number, expiry date, CVV, details related to the merchant device such as device address to identify the merchant, etc. received in the encoded form) and customer delegate mobile device identification information (e.g., Bluetooth address of the smartphone). See Ex. B. The card reader stores the credit card number, Bluetooth address of the smartphone in its memory to complete the delegated transaction. See Ex. B.

34. As recited in one step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls subsequent to acquiring customer delegate mobile device identification information (e.g., Bluetooth address of the smartphone) and secure transaction data (e.g., Data required to complete the delegated transaction

such as Credit Card number, expiry date, CVV, details related to the merchant device such as device address to identify the merchant, etc. received in the encoded form) by the customer secure computing device (e.g., card reader), automatically completing the secure transaction, by the customer secure computing device (e.g., card reader), in response to receiving a communication (e.g., authentication for the delegated transaction via customer's signature) from the identified previously authorized customer delegate mobile device (e.g., smartphone). See Ex. B. After the card reader receives the authentication for the delegate transaction via customer's signature from the smartphone, it automatically starts initiating payment to the merchant. See Ex. B.

35. As recited in another step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls receiving, by the customer secure computing device (e.g., card reader), a communication (e.g., authentication for the delegated transaction via customer's signature) from the identified previously authorized customer delegate mobile device (e.g., smartphone). See Ex. B.

36. As recited in one step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls checking, by the customer secure computing device, a status identifier in the communication (e.g., authentication for the delegated transaction via customer's signature) from the identified previously authorized customer delegate mobile device (e.g., smartphone). See Ex. B.

37. As recited in another step of Claim 1, the system, at least in internal testing and usage, utilized by the Accused Product practices and/or directs or controls automatically initiating, by the customer secure computing device (e.g., card reader), using the secure transaction data (e.g., Data required to complete the delegated transaction such as Credit Card number, expiry date, CVV, details related to the merchant device such as device address to identify the merchant, etc. received

in the encoded form), payment to the merchant by the customer secure computing device in response to receiving the communication (e.g., authentication for the delegated transaction via customer's signature) from the identified previously authorized customer delegate mobile device (e.g., smartphone), when the status identifier indicates that the delegated transaction (e.g., current transaction or transaction in discussion) is complete (e.g., when the authentication from the smartphone is completed, delegated transaction is automatically initiated to be transferred to the merchant account). See Ex. B. After the card reader receives the authentication for the delegate transaction via customer's signature from the smartphone, it automatically starts initiating payment to the merchant. The payment only initiates to the merchant when the signature is correctly received. See Ex. B.

38. The elements described in the preceding paragraphs are covered by at least Claim 1 of the '165 Patent. Thus, Defendant's use of the Accused Product is enabled by the method described in the '165 Patent.

INFRINGEMENT OF THE PATENT-IN-SUIT

39. Plaintiff realleges and incorporates by reference all of the allegations set forth in the preceding paragraphs

40. In violation of 35 U.S.C. § 271, Defendant is now, and has been directly infringing the '165 Patent.

41. Defendant has had knowledge of infringement of the '165 Patent at least as of the service of the present Complaint.

42. Defendant has directly infringed and continues to directly infringe at least one claim of the '165 Patent by using, at least through internal testing or otherwise, the Accused Product without authority in the United States, and will continue to do so unless enjoined by this

Court. As a direct and proximate result of Defendant's direct infringement of the '165 Patent, Plaintiff has been and continues to be damaged.

43. Defendant has contributed to and induced others to infringe the '165 Patent by encouraging infringement, directing or controlling, knowing that the acts Defendant induced constituted patent infringement, and its encouraging acts that direct or control others to directly infringe the '165 patent.

44. By engaging in the conduct described herein, Defendant has injured Plaintiff and is thus liable for infringement of the '165 Patent, pursuant to 35 U.S.C. § 271.

45. Defendant has committed these acts of infringement without license or authorization.

46. As a result of Defendant's infringement of the '165 Patent, Plaintiff has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate for Defendant's past infringement, together with interests and costs.

47. Plaintiff will continue to suffer damages in the future unless Defendant's infringing activities are enjoined by this Court. As such, Plaintiff is entitled to compensation for any continuing and/or future infringement up until the date that Defendant is finally and permanently enjoined from further infringement.

48. Plaintiff reserves the right to modify its infringement theories as discovery progresses in this case; it shall not be estopped for infringement contention or claim construction purposes by the claim charts that it provides with this Complaint. The claim chart depicted in Exhibit B is intended to satisfy the notice requirements of Rule 8(a)(2) of the Federal Rule of Civil Procedure and does not represent Plaintiff's preliminary or final infringement contentions or preliminary or final claim construction positions.

DEMAND FOR JURY TRIAL

49. Plaintiff demands a trial by jury of any and all causes of action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

a. That Defendant be adjudged to have directly infringed the '165 Patent either literally or under the doctrine of equivalents;

b. An accounting of all infringing sales and damages including, but not limited to, those sales and damages not presented at trial;

c. That Defendant, its officers, directors, agents, servants, employees, attorneys, affiliates, divisions, branches, parents, and those persons in active concert or participation with any of them, be permanently restrained and enjoined from directly infringing the '165 Patent;

d. An award of damages pursuant to 35 U.S.C. §284 sufficient to compensate Plaintiff for the Defendant's past infringement and any continuing or future infringement up until the date that Defendant is finally and permanently enjoined from further infringement, including compensatory damages;

e. An assessment of pre-judgment and post-judgment interest and costs against Defendant, together with an award of such interest and costs, in accordance with 35 U.S.C. §284;

f. That Defendant be directed to pay enhanced damages, including Plaintiff's attorneys' fees incurred in connection with this lawsuit pursuant to 35 U.S.C. §285; and

g. That Plaintiff be granted such other and further relief as this Court may deem just and proper.

Dated: March 29, 2021

Respectfully submitted,

/s/ Raymond W. Mort, III

Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
100 Congress Ave, Suite 2000
Austin, Texas 78701
Tel/Fax: (512) 865-7950

ATTORNEYS FOR PLAINTIFF

Together with:

SAND, SEBOLT & WERNOW CO., LPA

Howard L. Wernow
(*pro hac vice forthcoming)*

Aegis Tower – Suite 1100
4940 Munson Street NW
Canton, Ohio 44718
Telephone: (330) 244-1174
Facsimile: (330) 244-1173
Howard.Wernow@sswip.com